Techno.COM, Vol. 17, No. 4, November 2018 : 347-354

Realtime Pencegahan Serangan *Brute Force* dan DDOS Pada Ubuntu *Server*

Realtime Prevention of Brute Force and DDOS Attacks On Ubuntu Server

Syaifuddin[1], Diah Risqiwati[2], Eko Ari Irawan[3]
[1,2,3]Fakultas Teknik , Program Studi Teknk Informatika
Universitas Muhammadiyah Malang
Email: [1]saifuddin@umm.ac.id,[2]diah.rizqiwati@gmail.com, [3]ekoariirawan11@gmail.com

Abstrak

Dalam era globalisasi ini perkembangan internet semakin cepat dalam penggunaan internet semakin banyak dan informasi, data yang sangat penting sangat perlu di jaga, di sisi lain terdapat banyak resiko terhadap keamanan dalam sistem jaringan terutama web server, sementara asset yang ada dalam informasi tersebut perlu dilindungi karena banyak cara yang dilakukan oleh seorang hacker untuk mendapatkan informasi atau data yang penting karena semakin terbuka dalam pengetahuan hacking dan cracking, sehingga banyak beberapa pihak yang tidak bertanggung jawab mencoba untuk mencuri atau mengambil informasi, dengan di dukung banyaknya tools yang free, sehingga mempermudah para hacker dan attacker mencoba untuk melakukan aksi penyusupan maupun serangan. Seorang administrator membutuhkan sistem yang bisa membantu kinerjanya. Sebuah sistem yang bisa membantu administrator jika sedang tidak berada dalam kondisi di tempat, sebuah sistem yang dapat memberikan hasil laporan atau report secara realtime apa yang terjadi pada sistem apakah itu sebuah serangan atau penyusupan yang nantinya akan mempermudah kinerja seorang administrator dan bisa bertindak lebih jauh untuk mencegah terjadinya serangan di kemudian hari dan agar tidak terjadi upaya serangan atau penyusupan lagi.

Kata kunci : Bruteforce, DDOS, fail2ban, fail2sql

Abstract

In this era of globalization the rapid development of internet in the use of the internet more and more information, very important data need to be on guard, on the other hand there are many risks to the security in network systems, especially web server, while the assets in the information need to be protected because many the way that a hacker to get information or data that is important because it is more open in the knowledge of hacking and cracking, so many irresponsible parties try to steal or retrieve information, with the support of many tools that are free, making it easier for hackers and attacker tries to infiltrate and attack. one of them is ddos attacks. An administrator needs a system that can help his performance. A system that can help administrators if they are not in the on-site condition, a system that can deliver real-time reports or reports of what happens to the system whether it is an attack or infiltration that will facilitate an administrator's performance and can go further for prevent the occurrence of attacks in the future and so that no attempt to attack or infiltration again.

Keyword(s) *: Bruteforce, DDOS, fail2ban, fail2sql*

1. PENDAHULUAN

Perkembangan internet semakin cepat disisi lain semakin banyak informasi, data yang sangat penting sangat perlu dilindungi karena banyak cara yang dilakukan oleh seorang hacker untuk mendapatkan informasi atau data yang penting karena semakin terbukanya dalam pengetahuan hacking dan cracking, sehingga banyak beberapa pihak yang tidak bertanggung jawab mencoba untuk mencuri atau mengambil informasi,dengan di dukung banyaknya tools yang free,sehingga mempermudah para hacker dan attacker mencoba untuk melakukan aksi penyusupan maupun serangan.salah satu serangan ddos. Sehingga pada keamanan komputer, objek yang perlu dilindungi adalah komputer dan informasi[1].

Serangan brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung, dan dengan cara yang jelas. Penyelesaian permasalahan password cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan password dengan masukan karakter dan panjang password tertentu tentunya dengan banyak sekali kombinasi password [2]. Inilah yang mungkin menjadi alasan perlunya keamanan komputer atau keamanan informasi bagi sebuah organisasi. Menurut Charles P. Pfleeger, keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan oleh seorang hacker [3].

Maka dari permasalahan tersebut, seorang administrator membutuhkan sistem yang bisa membantu kinerjanya. Sebuah sistem yang bisa membantu administrator jika sedang tidak berada dalam kondisi di tempat, sebuah sistem yang dapat memberikan hasil laporan atau report apa yang terjadi pada sistem apakah itu sebuah serangan atau penyusupan. Fail2ban merupakan paket program untuk mendeteksi usaha login yang gagal dan kemudian memblokir alamat IP host asal [4], menurut Elinggwood Fail2ban bekerja dengan cara merubah aturan konfigurasi firewall dengan konfigurasi yang berada di Fail2ban itu sendiri, ketika Fail2ban berjalan, ia akan mengambil alih fungsi firewall yang berada di server [5]. Pada penelitian yang dilakukan oleh Suroto dan John Friadi yang berjudul "Membangun Sistem Kemanan Komputer Untuk Menghadapi Serangan Brute force Dengan Fail2ban" memberikan saran yang dapat disampaikan untuk penelitian selanjutnya, adalah penambahan keamanan pada service lain, seperti DNS, SMB dan lain-lain. Sehingga Fail2Ban dapat mencegah serangan Brute Force pada service tersebut [6]. Pada penelitian yang dilakukan oleh Iwan Kurniawan yang berjudul "Sistem Pencegahan Serangan BruteForce Pada Ubuntu Server Dengan Menggunakan Fail2ban" menyatakan bahwa Implementasi fail2ban pada Ubuntu server terbukti dapat mencegah serangan bruteforce dan memblokir alamat ip dari penyerang [7]. fungsi fail2ban itu sendiri untuk monitor jumlah kegagalan login ssh di server, yang selanjutnya ip akan diblokir sehingga mempermudah kinerja administrator, Fail2ban dapat mengamankan berbagai server dan kemudian memberikan hasil serangan berupa data log.

Dengan menggunakan program fail2sql mempermudah untuk menganalisa terjadi serangan karena program fail2sql mencatat log serangan pada fail2ban berupa ip address, port, protocol, dan waktu saat menyerang secara realtime, cara kerja program fail2sql ini adalah mengambil hasil log serangan pada fail2ban secara realtime. program *fail2sql* menggunakan bahasa pemograman *php* dan hasil dalam serangan log itu nanti seorang admin lebih mempermudah proses menganalisa dan membacanya dalam suatu terjadinya serangan terhadap server karena output mudah dibaca.

2. METODE PENELITIAN

Pada penelitian ini metode penelitian yang ditempuh dimulai dengan analisa kebutuhan, desain sistem, hasil dan pembahasan.

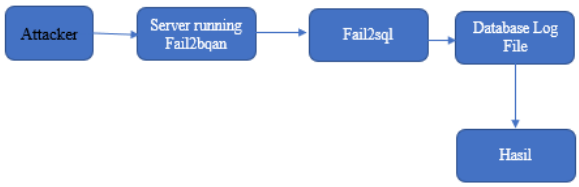
2.1 Analisa Kebutuhan

Pada tahap ini akan dilakukan identifikasi analisa terhadap kebutuhan sistem. Pengumpulan data dalam tahap ini bisa diperoleh dari penelitian, percobaan, konsultasi dengan pakar dan studi literatur. Berdasarkan studi literatur yang berhubungan dengan Fail2ban dapat dijelaskan bahwa *Fail2ban* merupakan salah satu aplikasi yang membantu administrator dalam mengamankan jaringan. Fail2ban beroperasi dengan memblokir IP yang mencoba melanggar keamanan sistem. Alamat IP yang diblokir dapat dilihat pada file log (misalnya: /var/log/pwdfail, /var/log/auth.log, dan lain-lain) dan melarang setiap IP yang berupaya login terlalu banyak atau melakukan tindakan yang tidak diinginkan lainnya dalam jangka waktu yang ditetapkan oleh administrator.

Untuk mendapatkan log dari setiap server perlu metode fail2sql untuk membungkus semua hasil log yang nantinya akan dikirim ke database dan hasil data dari database dalam semua paket log serangan pada server akan dibuat dalam bentuk highcharts sehingga proses analisa lebih mudah terbaca.

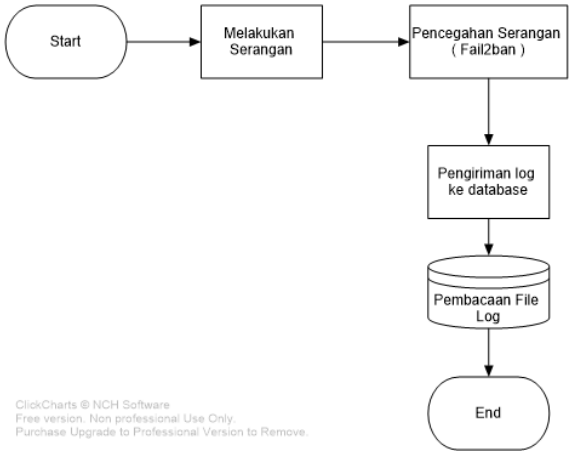
2.2 Desain System

Tahapan ini merupakan perancangan sistem terhadap solusi dari permasalahan yang ada dengan menggunakan perangkat pemodelan sistem seperti *block diagram* dan *flowchart*, pada *block diagram* akan digambarkan runtutan kinerja program pada penelitian ini, pada bagian *flowchart* akan menggambarkan alur program yang jalankan.



Gambar 1 *Block diagram sistem*

Pada Gambar 1 merupakan gambaran dari urutan attacker terhadap server. penggunaan fail2sql guna untuk mengirim hasil log fail2ban ke database secara realtime dan hasil log serangan yang tersimpan pada databse akan di krim dengan menggunakan Bahasa pemograman php dan nantinya hasil log dalam database, sehingga dalam pencegahan serangan ini dapat dianalisa.



Gambar 2. *Flowchart sistem*

Pada Gambar 2 merupakan flowchart program yang menggambarkan alur kerja program yang di tulis pada bahasa pemograman *php* yang bertugas mengambil file secara realtime dan membaca file dari database.dan nantinya di analisa.

3. HASIL DAN PEMBAHASAN

3.1 Design Network Architecture

Gambar 3 Desain Arsitektur Jaringan.

Server terinstall Ubuntu Server 14.04 dan beberapa program: OpenSSH dan Apache. Sedangkan pada host penyerang terinstall sistem operasi Kali Linux dan program hydra, medusa, xerves dan browser.

3.2. Instalasi Perangkat Lunak dan konfigurai fail2ban

Instalasi dan konfigurasi perangkat lunak meliputi Sistem Operasi, OpenSSH, Apache dan Fail2ban .

- Konfigurasi ssh pada fail2ban dengan perintah sudo nano /etc/fail2ban/jail.local

```
 GNU nano 2.2.6                File: jail.local

# Optionally you may override any other parameter (e.g. banaction,
# action, port, logpath, etc) in that section within jail.local

[ssh]

enabled  = true
port     = ssh
filter   = sshd
action   = %(action_mwl)s
logpath  = /var/log/auth.log
banaction = iptables

maxretry = 3
findtime = 300
bantime  = 300
```

Gambar 4 Konfigurasi ssh pada fail2ban

Disini konfigurasi ssh untuk mengatur rule dan membatasi jumlah kegagalan hingga batas waktu ip addres terblokir.

- Konfigurasi banaction ssh pada fail2ban dengan perintah sudo nano /etc/fail2ban/ action.d/iptables.conf

```
 GNU nano 2.2.6                File: iptables.conf

# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
            /usr/local/fail2sql/fail2sql <name> <protocol> <port> <ip>
# Option:  actionunban
```

Gambar 5 Konfigurasi banaction ssh pada fail2ban

Disini program fail2sql berjalan untuk mengambil log secara realtime terhadap serangan selanjutkan akan dikirim ke database.

- Konfigurasi apache (http) pada fail2ban dengan perintah sudo nano /etc/fail2ban/jail.local

Gambar 6 Konfigurasi apache pada fail2ban

Disini konfigurasi apache untuk mengatur rule dan membatasi jumlah kegagalan hingga batas waktu ip addres terblokir.

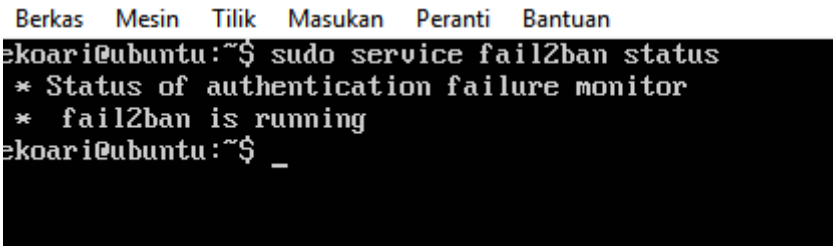
- Konfigurasi banaction ssh pada fail2ban dengan perintah sudo nano /etc/fail2ban/ action.d/iptables.conf

Gambar 7 Konfigurasi banaction apache pada fail2ban

Disini program fail2sql berjalan unutk mengambil log secara realtime terhada serangan selanjutkan akan dikirim ke database.

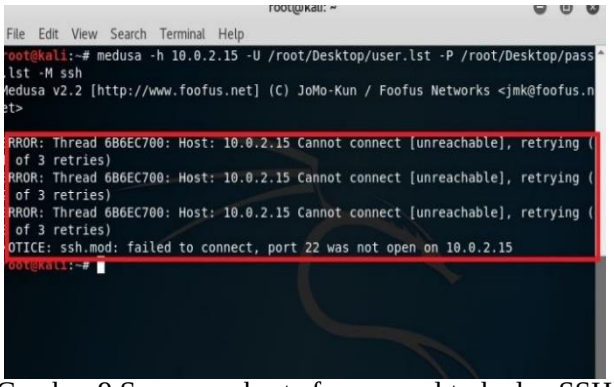
3.3. Simulasi dan ujicoba serangan.

Ujicoba serangan brute-force terhadap server dilakukan dalam saat fail2ban yang ada di server enabled. Serangan meliputi brute-force,ddos terrhadap SSH dan HTTP. Semua serangan dilakukan dari host attacker. Pada tahap I ujicoba, fail2ban dalam keadaan tidak berjalan, seperti gambar 3. Perintah yang digunakan yaitu, 'sudo service fail2ban status' .



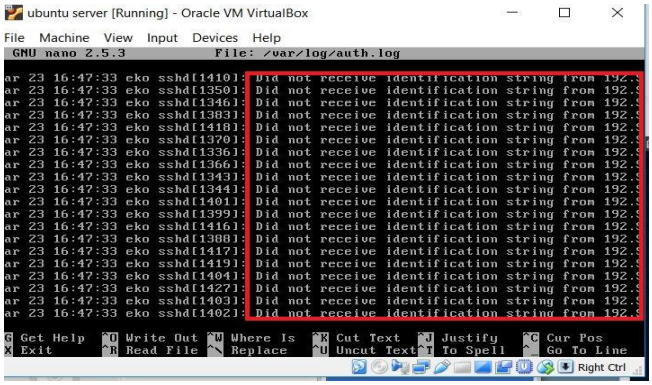
Gambar 8 Status Fail2ban Aktif

Ujicoba 1: Serangan Bruteforce pada SSH dilakukan dengan perintah sebagai berikut :
Medusa -h 10.0.2.15 -U /root/Desktop/userlist -p /root/Desktop/pass.list -M ssh.
Dimana Medusa adalah sebuah tool yang dilakukan untuk melakukan brute force attack dengan menggunakan sebuah dictionary atau list password untuk mencoba masuk.



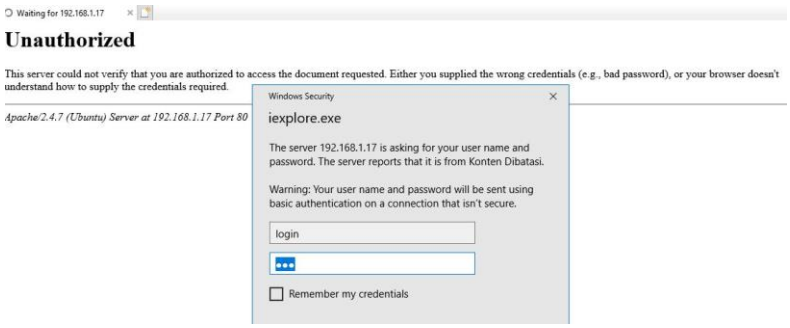
Gambar 9 Serangan brute force gagal terhadap SSH

Ujicoba 2: Serangan DDOS pada SSH dilakukan dengan perintah sebagai berikut :
./xerxes 192.168.1.9 22
Dimana tools xerxes adalah tools yang digunakan untuk serangan DDOS.



Gambar 10 Serangan DDOS gagal terhadap SSH

Ujicoba 3: Serangan bruteforce pada apache dilakukan dengan perintah sebagai berikut :

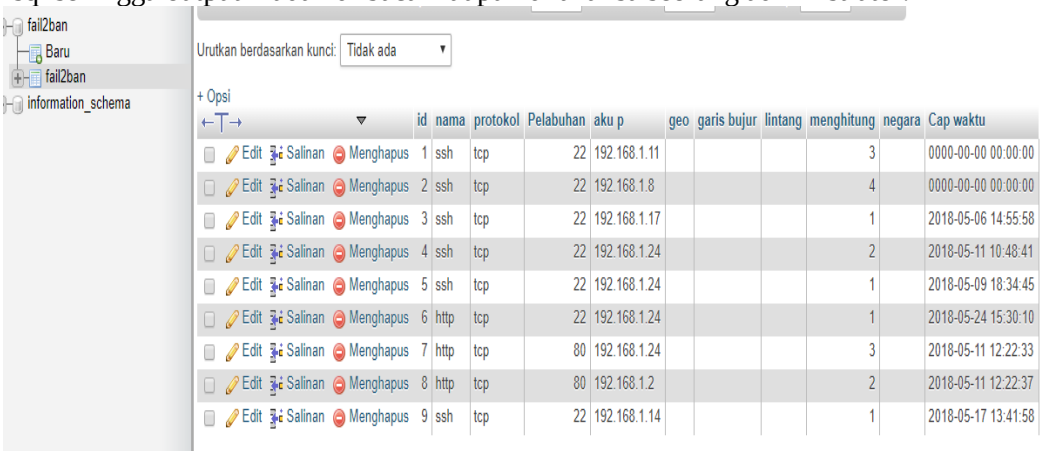


Gambar 11 Serangan Bruteforce terhadap apache

Berdasarkan hasil dari semua ujicoba serangan brute-force dan DDOS, menunjukkan bahwa:

1. Ketika fail2ban disable, semua serangan berhasil menemukan password yang valid.
2. Ketika fail2ban enabled, semua serangan tidak berhasil menemukan password yang valid

Hasil serangan dapat terbaca secara realtime dan tersimpan ke dalam database melalui program fail2sql sehingga output mudah di baca maupun di analisa seorang administrator.



Gambar 12 log serangan ke dalam database

Beberapa hasil yang di proses melalui fail2sql yang dapat dikirim ke dalam database. proses pengiriman ke database tidak semua log yang dikirim karena proses pengiriman ada parameter yang di buat agar log yang tidak berguna tidak masuk ke dalam database, di sini proses program fail2sql mempermudah pengiriman log dan menganalisa hasil log.

Tabel 1 Penjelasam program fail2ban dan fail2sql

Program	Percobaan	Output fail2ban	Output Database
Fail2ban	Ujicoba 1 ssh brutefoce	Ip address, jumlah kegagalan	-
	Ujicoba 2 ssh ddos	Ip address, jumlah kegagalan	-
	Ujicoba 3 apache bruteforce	Ip address, jumlah kegagalan	-
Fail2sql	Ujicoba 1 ssh brutefoce	-	Ip address, port, protocol, waktu
	Ujicoba 2 ssh ddos	-	Ip address, port, protocol, waktu
	Ujicoba 3 apache bruteforce	-	Ip address, port, protocol, waktu

4. KESIMPULAN

Kesimpulan dari penelitian untuk melakukan implementasi fail2ban pada Ubuntu server versi 16 untuk mencegah serangan bruteforce dan DDOS. Dengan menggunakan fail2ban dapat mencegah serangan bruteforce dan DDOS dan hasil serangan pada server lognya akan di krim ke database, proses pengiriman melalui program yang nantinya mengirim log sesusai parameter yang adalam dalam program. Dengan menggunakan fail2sql proses pengiriman log secara realtime karena program fail2sql berjalan pada saat ada serangan dan ip address terblokir secara langsung program fail2sql mengambil data serangan berupa ip address, port, protocol, waktu dan dikirim ke dalam database sehingga lebih mempermudah administrator menganalisa log dan lebih mudah di baca karena tidak semua log yang dikirim.

5. SARAN

Saran penelitian kedepannya menambahkan keamanan ke dalam jenis port lain pada server sehingga serangan terhadap server tidak dapat dilakukan oleh seorang attacker. Dan juga dapat menambahkan metode untuk menganalisa hasil log serangan, sehingga administrator tidak menganalisa secara manual.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Kepala Laboratorium Teknik Informatika yang telah memberikan ijin kepada penulis untuk melakukan riset tentang Realtime Pencegahan Serangan *Brute Force* dan *DDoS* ini.

DAFTAR PUSTAKA

[1] K. J.M, “Guide To Computer Security Third Edition,” Chattanooga: Springer, 2014.
[2] H. S. Pratita, “Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack,” *2016*.
[3] C. P. Pfleeger, “Security In Computing,” 5th editio., New York: Prentice Hall, 2015.
[4] Wikipedia, “Admin An Introduction.” [Online]. Available: http://www.fail2ban.org/wiki/index.php/ Main_Page. [Accessed: 20-Mar-2018].
[5] E. Justin, “How Fail2ban Works to Protect Services on Linux Server,” 2014. [Online]. Available: https://www.digitalocean.com/community/ tutorials/how-fail2ban-works-to-protectservices-on-a-linux-server. [Accessed: 20-Mar-2018].
[6] Suroso. “Membangun Sistem Kemanan Komputer Untuk Menghadapi Serangan Brute force Dengan Fail2ban .” Seminar Nasional Teknologi Informasi dan Komunikasi Terapan (SEMANTIK) 2015. http://www.slackerbox.com/node/552. [Accessed: 20-Mar-2018].
[7] Pleeger and J. Margulies. Security in Computing. Fifth Edition. New York: Pearson Education Inc. 2015